(ร่าง) หลักเกณฑ์ตามลักษณะของการให้บริการ

<u>เค้าโครงร่างหลักเกณฑ์</u>

หมวด 1 บริการพิสูจน์ตัวตน บริการออกและบริหารจัดการสิ่งที่ใช้ยืนยันตัวตน และบริการยืนยันตัวตน

ส่วนที่ 1 การพิสูจน์ตัวตน

ส่วนที่ 2 การออกและบริหารจัดการสิ่งที่ใช้ยืนยันตัวตน และการยืนยันตัวตน

ส่วนที่ 3 การเชื่อมโยงและแลกเปลี่ยนข้อมูล

ส่วนที่ 4 การพิสูจน์และยืนยันตัวตนโดยใช้เทคโนโลยีชีวมิติ

ส่วนที่ 5 การตรวจสอบประวัติการใช้งาน

หมวด 2 บริการแลกเปลี่ยนข้อมูลเพื่อการพิสูจน์และยืนยันตัวตนทางดิจิทัล

ส่วนที่ 1 ข้อกำหนดทั่วไป

ส่วนที่ 2 ข้อกำหนดด้านความสอดคล้องของระบบให้บริการ

ส่วนที่ 3 ข้อกำหนดด้านเทคนิค

(ร่าง) หลักเกณฑ์ตามลักษณะของการให้บริการ

หมวด 1
บริการพิสูจน์ตัวตน บริการออกและบริหารจัดการสิ่งที่ใช้ยืนยันตัวตน และบริการยืนยันตัวตน

ส่วนที่ 1 การพิสูจน์ตัวตน

1. ผู้รับใบอนุญาตต้องบริหารจัดการกระบวนการพิสูจน์ตัวตนให้สอดคล้องตามลักษณะและระดับความเสี่ยงของธุรกรรมหรือการประกอบธุรกิจ
2. ในการให้บริการพิสูจน์ตัวตน ผู้รับใบอนุญาตต้องมีกระบวนการที่ครอบคลุมการทำงานอย่างน้อยในเรื่องดังต่อไปนี้
   2.1 ต้องจัดให้ผู้ใช้บริการสามารถปรับปรุงข้อมูลเกี่ยวกับอัตลักษณ์ของตน ซึ่งถูกจัดเก็บในกระบวนการพิสูจน์ตัวตนได้ โดยต้องจัดให้มีกระบวนการตรวจสอบที่เกี่ยวข้องอย่างน้อยดังนี้
      (1) ตรวจสอบข้อมูลที่ขอปรับปรุงก่อนที่จะบันทึกการเปลี่ยนแปลงข้อมูลในระบบให้บริการ รวมถึงกรณีที่มีการเปลี่ยนแปลงสถานะของอัตลักษณ์ดิจิทัลนั้น เช่น การระงับชั่วคราว การใช้งานใหม่ เป็นต้น
      (2) ในกรณีที่ตรวจพบการทำธุรกรรมที่ผิดปกติ ต้องมีการตรวจสอบว่าอัตลักษณ์ดิจิทัล (Digital Identity) นั้น ยังอยู่ภายใต้ความควบคุมของเจ้าของอัตลักษณ์ดิจิทัลที่แท้จริง
   2.2 ในกรณีที่ผู้ใช้บริการร้องขอให้ระงับการใช้งานชั่วคราว (suspend for the period requested) หรือยุติการใช้งาน (deactivate) อัตลักษณ์ดิจิทัล ผู้รับใบอนุญาตต้องจัดให้มีกระบวนการอย่างน้อย ดังนี้
      (1) มีการตรวจสอบความถูกต้องของคำขอก่อนที่จะดำเนินการตามคำขอ
      (2) ป้องกันไม่ให้มีการใช้งานอัตลักษณ์ดิจิทัลตามคำขอ
      (3) มีการแจ้งให้ผู้ใช้บริการทราบว่าไม่สามารถใช้งานอัตลักษณ์ดิจิทัลได้ พร้อมระบุเหตุผล เช่น ระงับการใช้งานชั่วคราว ยุติการใช้งาน เป็นต้น
3. กรณีที่ระบบให้บริการรองรับการยกระดับความน่าเชื่อถือของการพิสูจน์ตัวตน ผู้รับใบอนุญาตต้องดำเนินการอย่างน้อย ดังนี้
   3.1 ต้องดำเนินการให้สอดคล้องตามข้อกำหนดระดับความน่าเชื่อถือของการพิสูจน์ตัวตนที่สูงกว่าให้ครบถ้วน
   3.2 ต้องจัดให้ผู้ใช้บริการยืนยันตัวตนด้วยสิ่งที่ใช้ยืนยันตัวตนของบุคคลนั้นก่อนเริ่มกระบวนการยกระดับความน่าเชื่อถือของการพิสูจน์ตัวตน
   3.3 เมื่อดำเนินการยกระดับความน่าเชื่อถือของการพิสูจน์ตัวตนเสร็จสิ้น ต้องส่งการแจ้งเตือนผู้ใช้บริการผ่านช่องทางที่เป็นอิสระจากช่องทางที่ใช้ยกระดับการพิสูจน์ตัวตนดังกล่าว เช่น การส่งให้ทางอีเมลของผู้ใช้บริการ
4. ผู้รับใบอนุญาตต้องจัดให้มีมาตรการดูแลข้อมูลผู้ใช้บริการอย่างน้อย ดังนี้
   4.1 ต้องรวบรวมหรือจัดเก็บข้อมูลเพื่อการพิสูจน์ตัวตนเพียงเท่าที่จำเป็น เหมาะสม และตรงตามวัตถุประสงค์ของการให้บริการ
   4.2 ต้องจำกัดการเปิดเผยข้อมูลอัตลักษณ์ของผู้ใช้บริการต่อบุคคลอื่นเพื่อใช้ในการพิสูจน์ตัวตนตามที่ได้รับความยินยอมจากผู้ใช้บริการ

ส่วนที่ 2 การออกและบริหารจัดการสิ่งที่ใช้ยืนยันตัวตน และการยืนยันตัวตน

5. ผู้รับใบอนุญาตต้องบริหารจัดการสิ่งที่ใช้ยืนยันตัวและการยืนยันตัวตนให้สอดคล้องตามตามลักษณะและระดับความเสี่ยงของธุรกรรมหรือการประกอบธุรกิจ
6. การบริหารจัดการสิ่งที่ใช้ในการยืนยันตัวตน ให้พิจารณาตามข้อกำหนดของการยืนยันตัวตน ตามมาตรฐานการพิสูจน์และยืนยันตัวตนทางดิจิทัล ซึ่งครอบคลุมกระบวนการอย่างน้อยดังนี้
   (1) การเชื่อมโยงสิ่งที่ใช้ยืนยันตัวตน
   (2) การสูญหาย ถูกขโมย เสียหาย และการออกทดแทน
   (3) การหมดอายุและการออกใหม่
   (4) การเพิกถอน หรือยุติการใช้งาน
7. ชนิดของสิ่งที่ใช้ยืนยันตัวตนและข้อกำหนดเกี่ยวกับสิ่งที่ใช้ยืนยันตัวตน ให้พิจารณาตามข้อกำหนดของการยืนยันตัวตน ตามมาตรฐานการพิสูจน์และยืนยันตัวตนทางดิจิทัล ซึ่งครอบคลุมหัวข้ออย่างน้อยดังต่อไปนี้
   (1) ชนิดของสิ่งที่ใช้ยืนยันตัวตนเพื่อใช้ในการยืนยันตัวตนตามระดับความน่าเชื่อถือของการยืนยันตัวตน (Authentication Assurance Level: AAL)
   (2) ข้อกำหนดทั่วไปของสิ่งที่ใช้ยืนยันตัวตน
8. ก่อนดำเนินการยืนยันตัวตน ผู้รับใบอนุญาตต้องตรวจสอบสิ่งที่ใช้ยืนยันตัวตนอย่างน้อยดังนี้
   8.1 ต้องตรวจสอบให้แน่ใจว่าสิ่งที่ใช้ยืนยันตัวตนที่แสดงนั้นถูกต้อง ใช้งานได้ และยังไม่หมดอายุหรือถูกเพิกถอน
   8.2 ในกรณีที่ตรวจพบการทำธุรกรรมที่ผิดปกติ ต้องมีการตรวจสอบว่าสิ่งที่ใช้ยืนยันตัวตนนั้น ยังอยู่ภายใต้ความควบคุมของเจ้าของ (อัตลักษณ์ดิจิทัล) ที่แท้จริง
   8.3 ในกรณีที่ผู้ใช้บริการร้องขอให้ระงับการใช้งานชั่วคราว (suspend for the period requested) หรือยุติการใช้งาน (deactivate) สิ่งที่ใช้ยืนยันตัวตน ผู้รับใบอนุญาตต้องจัดให้มี กระบวนการอย่างน้อยดังนี้
      (1) มีการตรวจสอบความถูกต้องของคำขอก่อนที่จะดำเนินการตามคำขอ
      (2) มีการแจ้งให้ผู้ใช้บริการทราบว่าไม่สามารถใช้งานสิ่งที่ใช้ยืนยันตัวตนได้พร้อมระบุเหตุผล เช่น ระงับการใช้งานชั่วคราว ยุติการใช้งาน เป็นต้น
9. กรณีที่ระบบให้บริการรองรับการยกระดับความน่าเชื่อถือของการยืนยันตัวตน ผู้รับใบอนุญาตต้องดำเนินการอย่างน้อย ดังนี้
   9.1 ต้องดำเนินการให้สอดคล้องตามข้อกำหนดระดับความน่าเชื่อถือของการยืนยันตัวตนที่สูงกว่าให้ครบถ้วน
   9.2 ต้องจัดให้ผู้ใช้บริการยืนยันตัวตนด้วยสิ่งที่ใช้ยืนยันตัวตนของบุคคลนั้นก่อนเริ่มกระบวนการยกระดับความน่าเชื่อถือของการยืนยันตัวตน
   9.3 เมื่อดำเนินการยกระดับความน่าเชื่อถือของการยืนยันตัวตนเสร็จสิ้น ต้องส่งการแจ้งเตือนผู้ใช้บริการผ่านช่องทางที่เป็นอิสระจากช่องทางที่ใช้ยกระดับการยืนยันตัวตนดังกล่าว (เช่น การส่งให้ทางอีเมลของผู้ใช้บริการ)

ส่วนที่ 3 การเชื่อมโยงและแลกเปลี่ยนข้อมูล

10. ผู้รับใบอนุญาตต้องกำหนดโพรโทคอลที่ใช้สำหรับการเชื่อมโยงและแลกเปลี่ยนข้อมูลในระบบให้บริการ (Communication protocol) ซึ่งครอบคลุมอย่างน้อย ดังนี้
    10.1 กำหนดโพรโทคอล (Protocol) สำหรับเชื่อมโยงคำขอ (request) และการตอบกลับ (response) โดยต้องสามารถเชื่อมโยงคำขอไปยังปลายทางที่ระบุโดยผู้ส่งคำขอได้ และสามารถเชื่อมโยงการตอบกลับไปยังคำขอต้นทางได้ (original request)
    10.2 กำหนดวิธีการเชื่อมต่อ (Application Programming Interface) ที่ใช้สำหรับการเชื่อมโยงและแลกเปลี่ยนข้อมูลเกี่ยวกับการพิสูจน์และยืนยันตัวตนในระบบให้บริการ โดยอย่างน้อยต้องสามารถเชื่อมโยงและจับคู่ (mapping) รายการต่อไปนี้เข้าด้วยกันได้อย่างถูกต้องและครบถ้วน
        (1) รายการข้อมูลที่กำหนดในคำขอและการตอบกลับ
        (2) ระดับความน่าเชื่อถือของการพิสูจน์และยืนยันตัวตนทางดิจิทัล (Assurance level) ตามที่กำหนดในคำขอและการตอบกลับ (Mapping assurance level)
11. ผู้รับใบอนุญาตต้องจัดทำนโยบายการเปิดเผยข้อมูลอัตลักษณ์ ที่สอดคล้องกับหลักเกณฑ์การคุ้มครองข้อมูลส่วนบุคคล และประกาศให้ผู้ที่เกี่ยวข้องได้รับทราบเป็นการทั่วไป
12. ผู้รับใบอนุญาตต้องจัดให้มีรายการข้อมูลอัตลักษณ์ที่ใช้สำหรับการเชื่อมโยงและแลกเปลี่ยนข้อมูลเกี่ยวกับการพิสูจน์และยืนยันตัวตนทางดิจิทัลในระบบให้บริการ โดยต้องมีชุดข้อมูลขั้นต่ำที่สามารถระบุตัวผู้ใช้บริการได้อย่างชัดเจน ประกอบด้วย
    (1) เลขประจำตัวประชาชน
    (2) ชื่อ นามสกุล ภาษาไทย
    (3) ชื่อ นามสกุล ภาษาอังกฤษ (ถ้ามี)
    (4) วัน เดือน ปี เกิด
    (5) ที่อยู่ตามบัตรประชาชน
13. ในการส่งผลการพิสูจน์และยืนยันตัวตน ผู้รับใบอนุญาตต้องดำเนินการอย่างน้อยดังนี้
    13.1 ผลการยืนยันตัวตน ประกอบด้วย ผลการตรวจสอบสิ่งที่ใช้ยืนยันตัวตน และข้อมูลเกี่ยวกับอัตลักษณ์ของผู้ใช้บริการ
    13.2 ต้องจัดให้มีการรักษาความลับของผลการพิสูจน์และยืนยันตัวตนในกระบวนการส่งผลการยืนยันตัวตน เพื่อให้มั่นใจว่าเฉพาะผู้อาศัยการยืนยันตัวตน (RP) เท่านั้นที่สามารถเข้าถึงข้อมูลได้
    13.3 ต้องส่งผลการพิสูจน์และยืนยันตัวตนผ่านช่องทางที่มีความมั่นคงปลอดภัย เพื่อรักษาความครบถ้วนของผลการพิสูจน์และยืนยันตัวตน
14. ห้ามมิให้ผู้รับใบอนุญาตส่งข้อมูลที่ใช้สำหรับการตรวจสอบสถานะของหลักฐานแสดงตนให้กับบุคคลอื่น โดยข้อมูลดังกล่าวได้แก่
    (1) เลขคำร้องขอมีบัตรประจำตัวประชาชน
    (2) หมายเลขชิปบัตรประจำตัวประชาชน
    (3) เลขควบคุมหลังบัตรประชาขน (เลเซอร์ ไอดี (Laser ID))

ส่วนที่ 4 การพิสูจน์และยืนยันตัวตนโดยใช้เทคโนโลยีชีวมิติ

15. ในกรณีที่มีการใช้งานข้อมูลชีวมิติในกระบวนการพิสูจน์และยืนยันตัวตน ต้องมีการดำเนินการ อย่างน้อย ดังนี้

15.1 ผู้รับใบอนุญาตต้องจัดให้มีการกำกับดูแลการใช้งานเทคโนโลยีชีวมิติตามหลักปฏิบัติ ดังนี้

(1) มีนโยบายและแนวปฏิบัติการนำเทคโนโลยีชีวมิติมาใช้ในการให้บริการอย่างชัดเจน ซึ่งต้องคำนึงถึงการดำเนินงานที่สำคัญอย่างน้อย ดังนี้

(1.1) การประเมินความเสี่ยงการนำเทคโนโลยีชีวมิติมาใช้ในการให้บริการ

(1.2) การปฏิบัติตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล และ

(1.3) การรักษาความมั่นคงปลอดภัยข้อมูลชีวมิติ

(2) มีการบริหารจัดการอัตลักษณ์เพื่อการพิสูจน์ตัวตนด้วยเทคโนโลยีชีวมิติที่สอดคล้องตามมาตรฐานการใช้งานเทคโนโลยีชีวมิติสำหรับการพิสูจน์และยืนยันตัวตน

(3) มีการจัดทำคู่มือหรือแนวปฏิบัติสำหรับบุคลากรที่ปฏิบัติงานเกี่ยวกับการใช้งานข้อมูลชีวมิติ

(4) มีการจัดทำคู่มือหรือการให้คำแนะนำผู้ใช้บริการในการใช้งานข้อมูลชีวมิติ

15.2 ต้องจำกัดการเข้าถึงการควบคุมข้อมูลชีวมิติ ให้สามารถเข้าถึงได้เฉพาะบุคลากรที่เกี่ยวข้องซึ่งผ่านการฝึกอบรมอย่างเหมาะสม และมีการสอบทานสิทธิอย่างสม่ำเสมอ

ส่วนที่ 5 การตรวจสอบประวัติการใช้งาน

16. ให้ผู้รับใบอนุญาตจัดเก็บข้อมูลประวัติการใช้งานเพื่อประโยชน์ในการสอบทานของผู้ใช้บริการ โดยต้องจัดเก็บไว้ในลักษณะที่พร้อมให้ผู้ใช้บริการเรียกดูข้อมูลย้อนหลังได้ทันที เป็นระยะเวลาไม่น้อยกว่าหกเดือน โดยอย่างน้อยควรมีข้อมูลที่ผู้ใช้บริการสามารถตรวจสอบได้ ดังต่อไปนี้

(1) ประวัติกิจกรรมของผู้ใช้บริการที่ได้ดำเนินการผ่านบริการของผู้รับใบอนุญาต

(2) ประวัติการให้ความยินยอมในการเปิดเผยข้อมูลอัตลักษณ์

17. การแสดงผลการตรวจสอบประวัติการใช้งาน ต้องไม่มีการแสดงข้อมูลส่วนบุคคลของผู้ใช้บริการ

หมวด 2
บริการแลกเปลี่ยนข้อมูลเพื่อการพิสูจน์และยืนยันตัวตนทางดิจิทัล

ส่วนที่ 1 ข้อกำหนดทั่วไป

18. ผู้รับใบอนุญาตต้องจัดให้มีมาตรการดูแลข้อมูลส่วนบุคคลอย่างน้อย ดังนี้

(1) ไม่นำข้อมูลส่วนบุคคลของผู้ใช้บริการมาใช้เป็นตัวระบุ (identifier) ผู้ใช้บริการ

(2) ไม่จัดเก็บหรือคงไว้ซึ่งข้อมูลส่วนบุคคลของผู้ใช้บริการที่มีการส่งจากผู้รับใบอนุญาตไปยังผู้อาศัยการพิสูจน์และยืนยันตัวตน เว้นแต่ เป็นการจัดเก็บโดยมั่นคงปลอดภัยในระหว่างเซสชัน (session) การพิสูจน์และยืนยันตัวตน และข้อมูลดังกล่าวต้องไม่สามารถเข้าถึงได้โดยบุคลากรของผู้รับใบอนุญาต

19. ผู้รับใบอนุญาตต้องจัดให้มีการบันทึกประวัติกิจกรรม (log) สำหรับบริการแลกเปลี่ยนข้อมูลเพื่อการพิสูจน์และยืนยันตัวตนทางดิจิทัล ดังนี้

(1) ต้องมีการกำหนดรหัสเฉพาะ (unique audit id) สำหรับคำขอเพื่อการยืนยันตัวตน (authentication request) ทุกรายการ เพื่อใช้เป็นตัวระบุเฉพาะสำหรับกิจกรรมการโต้ตอบ โดยการจัดเก็บบันทึก

ประวัติกิจกรรมการโต้ตอบที่เกิดขึ้นระหว่างกันให้ใช้รหัสเฉพาะเพื่อการตรวจสอบ (unique audit id) ที่กำหนดขึ้น

(2) ในการบันทึกประวัติกิจกรรม (Audit Logs) เกี่ยวกับการให้ความยินยอมของเจ้าของข้อมูล (ตามข้อกำหนดด้านข้อมูลส่วนบุคคล) ต้องจัดเก็บข้อมูลอย่างน้อย ดังต่อไปนี้

(2.1) เวลา

(2.2) ชื่อของระบบหรือผู้ร้องขอข้อมูล

(2.3) ตัวระบุ (identifier) ระบบหรือผู้ร้องขอข้อมูล

(2.4) ชื่อของระบบหรือผู้ให้ข้อมูล

(2.5) ตัวระบุ (identifier) ระบบหรือผู้ให้ข้อมูล

(2.6) รายการข้อมูลอัตลักษณ์ที่เกี่ยวข้อง

ส่วนที่ 2 ข้อกำหนดด้านความสอดคล้องของระบบให้บริการ

20. ในการกำหนดเงื่อนไขความสอดคล้องของเพื่อให้บุคคลอื่นสามารถเชื่อมต่อกับระบบให้บริการของผู้รับใบอนุญาตได้อย่างมีประสิทธิภาพ ผู้รับใบอนุญาตต้องแจ้งให้ผู้เชื่อมต่อทราบเกี่ยวกับเงื่อนไขความสอดคล้องของระบบให้บริการอย่างน้อยในเรื่องดังต่อไปนี้
    (1) ระดับความน่าเชื่อถือของการพิสูจน์และยืนยันตัวตนทางดิจิทัล (Assurance level) ที่สามารถเชื่อมต่อกับระบบให้บริการ
    (2) โพรโทคอล (Protocol) สำหรับเชื่อมโยงคำขอ (request) และการตอบกลับ (response) ในระบบให้บริการของผู้รับใบอนุญาต
21. ในการกำหนดความสอดคล้องของระดับความน่าเชื่อถือของการพิสูจน์และยืนยันตัวตนทางดิจิทัล ผู้รับใบอนุญาตต้องพิจารณาดำเนินการอย่างน้อย ดังนี้
    (1) จัดให้มีรายชื่อ และระดับความน่าเชื่อถือของการพิสูจน์และยืนยันตัวตนของผู้รับใบอนุญาตเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลที่เชื่อมต่อกับระบบให้บริการของตน
    (2) จัดให้มีกลไกที่สามารถคัดแยกผู้รับใบอนุญาตเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลที่เชื่อมต่อกับระบบให้บริการที่มีระดับความน่าเชื่อถือของการพิสูจน์และยืนยันตัวตนทางดิจิทัล (Assurance level) ในระดับที่สอดคล้องตามคำขอหรือสูงกว่าคำขอของผู้ส่งคำขอได้
22. การกำหนดโพรโทคอลที่ใช้สำหรับการเชื่อมโยงและแลกเปลี่ยนข้อมูลในระบบให้บริการ (Communication protocol) ให้ผู้รับใบอนุญาตดำเนินการตามหลักเกณฑ์ที่กำหนดในหมวดที่ 1 ส่วนที่ 3

ส่วนที่ 3 ข้อกำหนดด้านเทคนิค

23. ผู้รับใบอนุญาตต้องจัดให้มีแผนการทดสอบ (Testing Plan) การเชื่อมโยงและแลกเปลี่ยนข้อมูลบนระบบให้บริการ ที่สอดคล้องกับนโยบายการรักษาความมั่นคงปลอดภัยของระบบให้บริการ โดยแผนการทดสอบดังกล่าวเป็นส่วนหนึ่งของรายงานผลการตรวจประเมินความพร้อมในการประกอบธุรกิจ
24. ผู้รับใบอนุญาตต้องจัดให้มีการทดสอบการใช้งานตามแผนการทดสอบร่วมกับผู้ประสงค์จะเชื่อมต่อก่อนเริ่มให้บริการแก่บุคคลดังกล่าว
25. ห้ามมิให้เปิดให้บริการแก่ผู้ประสงค์จะเชื่อมต่อกับระบบให้บริการของผู้รับใบอนุญาตที่ไม่สามารถทดสอบการใช้งานร่วมกันกับผู้รับใบอนุญาตได้ หรือผลการทดสอบไม่สามารถดำเนินการได้โดยสมบูรณ์